FROM SEMAPHORE TO PREDATOR
Intelligence in the Internet Era

Remarks as prepared for delivery by

A. Denis Clift
President
Joint Military Intelligence College

Yale University
April 27, 2002

During the Napoleonic Wars, the French revolutionized land-based communications with the erection of semaphore towers bearing rotating arms to fashion coded signals that could speed line-of-sight from tower to tower along the coast and across the country at some 200 miles an hour. The British quickly followed suit in this new era of signals intelligence. Theft of the enemy's semaphore code books became an important part of the business of war.[1]

During the war on terrorism in Afghanistan, Predator unmanned aerial vehicles have been flying lengthy missions at heights of some 25,000 feet providing multi-hour surveillance of designated geography, installations, and activity. Tasking to the Predator and electro-optical video and infrared images collected by its cameras move near-instantaneously – which is to say real-time – to and from the area being surveilled and in-theater commanders and Washington. Communications and the resulting data stream flow through a network of ground stations and satellites with part of the product traveling through the secure medium of Intelink, the classified Internet counterpart.[2]

The episodic, manned U-2 photography missions of the 1950s; the periodic, evolutionary satellite photography missions proceeding from the 1960s have now been joined by the current generation of surveilling UAV eyes. Imaging collection, analysis, and decision-making that once proceeded in distinct, often lengthy sequential steps are now the business of simultaneity.

To leap thus across the centuries and the more recent decades is to realize in a glimpse the incredible dynamic involved in the world of intelligence and its supporting communications technologies. Actionable information from wherever on the face of the globe is today the air we breathe, essential to our national security and survival.

The Internet era is a dynamic with an on-rush of changes both revolutionary and far more subtle to the work of intelligence: changes in the doctrine and practice of collection, analysis, and dissemination; and changes in the relationship and the mindset between intelligence and law enforcement, intelligence and the policy-maker, and intelligence and the military commander.

ARPANET

In 1957, the communications signals from the beeping Soviet satellite Sputnik I would sound the beginning of the highly visible superpower space race. That race would produce some remarkable by-products – from cordless power tools and Teflon, to CAT Scanners and Magnetic Resonance Imaging technology. Out of the public eye, the orbiting Sputnik would launch other races by U.S. scientists and engineers. The United States realized that it must surge in its science programs. The Office of Science Adviser was added to the White House. In 1958, President Eisenhower created the Advanced Project Research Office, and that office as one of its earliest priorities tackled the challenge of linking research centers with one another and with their important sponsor, the Department of Defense.

As this research evolved, the computer's initial role as arithmetic engine would be joined by the computer as communications medium. Pioneers in the work of data networking and packet switching would bring their talents to the goal of the government-supported computer data network – ARPANET. Those pioneering the first network of the late 1960s – sites at UCLA, Stanford Research Institute, University of California Santa Barbara, and the University

of Utah – could not imagine their work would spawn the global Internet of today, to include the World Wide Web browser of the early l990s.[3]

This early ARPANET linkage work led to attention to another critical problem. If the Soviets could orbit Sputnik, who was to say that they were not now proceeding to develop the capability for space-based missile attack? A principal U.S. concern lay in the vulnerability of the nation's strategic communications infrastructure. If a nuclear attack destroyed key command and control centers, it would eliminate our ability to assess the impact of the attack and to decide on and deliver the strategic response. Attention would subsequently turn to fashioning a survivable computer network linking the Pentagon and the national decision-makers in Washington, with the Cheyenne Mountain nuclear command and control center and the Headquarters of the Strategic Air Command.[4]

The Chairman of my College's Board of Visitors, Dr. Anthony Oettinger, has written of the Information Technology/Internet era: "What it all boils down to is that faster, smaller, cheaper electro-optical digital technologies have put into our hands enormously powerful and varied yet increasingly practical and economical means for information processing, means that stimulate us to re-examine everything we do to information and with information, and then choose to do nothing, to reinforce the old ways, to modify them, or to abandon them altogether in favor of altogether new ways."[5] For U.S. intelligence, it is increasingly an era of modifications and altogether new ways. The technologies supporting U.S. intelligence develop in Web years, with three months to the Web year. The year 2010 is 32 Web years away.

Intelink & In-Q-Tel

If we are to consider key aspects of the play of intelligence in the Internet era, we should bear in mind at the outset that the U.S. Intelligence Community has developed and implemented

its own highly advanced, ever-evolving Intelink intranet, a secure collection of networks employing Web-based technology, using standard Web browsers such as *Navigator* and Internet *Explorer*. Intelink uses advanced network technology and applies it across the work of the departments and agencies of the Intelligence Community to the collection, analysis, production and dissemination of classified and unclassified multimedia data.[6]

In the assessment of the former Deputy Director of Central Intelligence, Admiral William O. Studeman, "Application of evolving Internet technologies to intelligence applications in the form of Intelink has been a transcendent and farsighted strategy. … Its future application requirements parallel those of the global Internet, so that there is the expectation that, for continuing modest investment, intelligence can continue to ride the wave of Internet growth, with commensurate access to amazing and relevant commercial off-the-shelf (COTS) developments. …"[7]

The Intelink intranet provides connectivity to national, theater, and tactical levels of government and military operations. Taking into account the sensitivity of some of the intelligence data involved, the sensitivity of the sources and methods for acquiring such data, the resulting 'need to know' of those logging on the system, Intelink provides several separate classification families, or instantiations of services. These range from:

-- Intelink-SCI, which operates at the top secret, compartmented intelligence level;

-- to the Intelink-PolicyNet, run by the Central Intelligence Agency as CIA's sole-source link to the White House and other high-level, intelligence consumers;

-- to Intelink-S, the SIPRnet at the secret level – the main communications link for the military commands and those operating land, sea and air; and

-- Intelink Commonwealth, or Intelink-C, linking the United States, United Kingdom, Canada, and Australia.[8]

A steadily evolving suite of Intelink support services, such as collaboration tools, search tools, and search engines, are available. Intelink security policy and practice reserving the intranet for authorized users, from encryption, to passwords, to user certifications and audits, are multi-layered and comprehensive.

In positioning itself for the Internet era, the Intelligence Community has gone beyond innovative use of the World Wide Web and its engines, to CIA's creation in 1999 of a private, not-for-profit company, In-Q-Tel, dedicated to spurring the development of information technologies to be used in the safeguarding of national security. As stated on its web page, "…the blistering pace at which the IT [information technology] economy is advancing has made it difficult for any government agency to access and incorporate the latest in information technology. In-Q-Tel strives to extend the Agency's access to new IT companies, solutions, and approaches to address their priority problems."[9]

In investing in technologies that can benefit CIA and the rest of the U.S. Intelligence Community at the same time that they will become available commercially, In-Q-Tel underscores that in this new era, underlying information technologies of importance to commerce are of importance to intelligence, IT functions such as data warehousing and mining, the profiling of search agents, statistical data analysis tools, imagery analysis and pattern recognition, language translation, strong encryption, data integrity, and authentication and access control. The work of In-Q-Tel, unclassified work with commercial potential, is giving initial attention to such issues as secure receipt of Internet information, non-observable surfing, hacker resistance, intrusion detection, data protection, and multimedia data fusion and integration.[10]

New Strengths for New Challenges

What are the goals being set for U.S. intelligence with this on-rushing development and implementation of information technology? For the Director of Central Intelligence, it is the goal of "a unified Intelligence Community optimized to provide a decisive information advantage to the President, the military, diplomats, the law enforcement community and the Congress."[11]

For the Chairman of the Joint Chiefs of Staff, as stated in *Joint Vision 2010*, it is, in parallel, the emerging importance of information superiority, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[12]

The need for information advantage, information superiority is in many instances causing U.S. intelligence to pursue dramatically new ways. The Internet era has become the Intelligence Community's new strength and its new challenge. The 46-year Cold War assumptions driving intelligence doctrine and practice – collection and analysis against closed society targets and subject matter in the superpower rivalry with the Soviet Union – are assumptions of the past.

If the semaphore was the signals intelligence breakthrough at the time of Napoleon, the Internet and its communications channels are at the forefront of signals intelligence challenges in this new century. With new transnational adversaries – the international terrorist foremost among them – with the flood of new information technologies, the easing of encryption export controls and global access to the Web, the National Security Agency is charting new directions in the ways it identifies, gains access to and successfully exploits target communications. NSA is also charting new ways of charting our information security, given the openness of our society

early in the cyber era, the global dimensions of that openness, and the enhanced exploitation capabilities that information technology and the Internet give our adversaries.

The Director of NSA, Lieutenant General Michael Hayden, has placed this challenge in the following context: "Forty years ago, there were 5,000 stand-alone computers, no fax machines and not one cellular phone. Today, there are over 180 million computers – most of them networked. There are roughly 14 million fax machines and 40 million cell phones and those numbers continue to grow, the telecommunications industry is making a $1 trillion investment to encircle the world in millions of high bandwidth fiber-optic cable."[13] At the same time, General Hayden reminds, the new information technologies are an enhancement and an enabler, as NSA seeks outs and exploits the current era's targets.

The Web and the new information technologies are an incredible enabler and at the same time a challenge to the intelligence analyst with a thousand different shadings depending on the specific work of the analyst and the consumer being served. To cite an example drawing on my own career experience as a policy-level consumer of intelligence, from 1974 to 1977, I was the head of President Ford's National Security Council staff for the Soviet Union and Eastern and Western Europe. As we pursued our nation's agenda with the USSR and Warsaw Pact, we were dealing with closed societies. There was no Web. The information being volunteered by the USSR was not usually the information we required. Intelligence collection, analysis, and dissemination were geared to ascertaining the current state of play and to estimating future developments behind the Iron Curtain. The role of the Intelligence Community's Sovietologists, the analysts expert on the USSR, was central. Not only could they divine the significance of any changes in the renowned line-up of the Soviet leadership atop Lenin's tomb, they often were the only source of information on developments of importance inside the Soviet Union.

The sources of information available to today's policy-level consumer – whether dealing with the Russian Federation or with any of the current closed societies – are far, far greater than a quarter century ago. It is almost a given that today's policy-level consumer of intelligence is quite well-informed in his or her area of interest and not dependent on an analyst for a continuing stream of routine, updating information. The analyst no longer sets the pace of the information flow. The Web, the media, electronic and hard-copy, U.S. and foreign, the telephone, the fax, the interaction with U.S. and foreign colleagues in the field, and intelligence reporting available at the touch of the Intelink keyboard all play a part.

Today's analyst must not only have a sense of his or her consumer's level of continuing information and knowledge. To provide value-added analysis, today's analyst must focus more sharply on the specific needs and the timing of meeting those needs for the policy-level consumer, seek specific tasking, analyze feedback from analysis already provided, and invite and tackle the consumer's hard questions demanding answers.[14]

NIST & the Joint Intelligence Virtual Architecture

If the policy-level consumer is demanding, in this new era, the military commander has, since the time of the late 1990s operations in the Balkans, been expecting the information superiority envisioned in *Joint Vision 2010*. The requirement, from mission planning through mission execution is for intelligence to be able to locate and to surveil targets either stationary or mobile, either exposed or hidden – to be able to obtain and provide to the commander a continuing picture of his entire field of operations in all its dimensions.

This extraordinary challenge requires intelligence to move fluidly to and from the national level, the theater commander in chiefs and the tactical commanders land, sea, and air. For any given requirement, the broadest capabilities of U.S. intelligence are considered

potentially available to contribute to the solution. The challenge posed by today's commander requires a complex harnessing of collection, analysis, and dissemination across the disciplines of intelligence – imagery, measurements and signatures, signals intelligence, human-source intelligence – to provide an as-valuable-as-possible all-source intelligence product when and where needed.

To say the least this commander's challenge to intelligence has not been universally met. Like Mount Everest, the challenge is there, and U.S. intelligence is ascending month after month, year after year with no little success. National Intelligence Support Teams, NIST teams, were born as a lesson learned from the U.S. participation in the DESERT STORM coalition that expelled Iraq from Kuwait. The teams belong to the Chairman of the Joint Chiefs of Staff's Director of Intelligence. When they deploy they are attached to the commander in the field. The idea is to provide the Joint Task Force commander with the ability to reach back swiftly, efficiently, and expertly to the national level agencies for answers to questions unanswerable in the field, and to receive warnings of threats that otherwise could not be received. NIST teams are fast-response, rapidly deployable intelligence cells made up of personnel from CIA, NSA, DIA and the National Imagery and Mapping Agency (NIMA). Using its light-weight, high-technology multi-media communications flowing via Intelink and satellite, the NIST team is able to link via voice, soft- and hard-copy word and imagery to bring the very best intelligence available to the commander in the field.[15] Truly, NIST is a remarkable advance in intelligence doctrine and methodology in the Internet era.

I have spoken more than once of the national, theater, and tactical levels. The world of the analyst in the Internet era is one in which collection and development of the analytic product, and its dissemination, are no longer limited to flow up and down hierarchical lines but move

horizontally and diagonally to selected nodes of the global intranet. The expert at the Joint Intelligence Center Pacific in Hawaii, for example, in the development of analysis may be routinely and matter-of-factly in Intelink contact with carrier battle group counterparts in the Indian Ocean and at the National Military Joint Intelligence Center at the Pentagon.

Collaborative information technology tools, using commercial web technologies, are being developed through the Joint Intelligence Virtual Architecture program to assist today's analyst in locating and accessing valuable data wherever it may be found, in assessing such data, in producing an informed analytic product, and in moving that product to where it will be of value. To cite a few examples, such tools are designed to provide search and discovery protocols allowing mining of data not only of what the analyst knows is important but also of – while unthought-of by the analyst – what might be of importance. Such tools will allow automatic extraction of relevant data from classified and unclassified sources. Such tools will support the analyst in making rapid assessments and developing time-critical reporting of streaming media – video and audio, for example.

Adding the enabling strengths of Web-based information technology to the analyst's kit is of importance for military intelligence if the commander is to have the continuing picture of the entire field of operations in all its dimensions. Such tools are of vital importance for analysts addressing asymmetric threats such as terrorism, where the disparate data must be located and mined not only from classified and unclassified intelligence sources, but also from worldwide open sources, and all in new and correct collaboration with the FBI, the INS, Customs, law enforcement both U.S. and international.

In 1899, Commissioner of Patents Charles Duell urged President William McKinley to abolish the Patent Office saying "Everything that can be invented has been invented." Those

fearless words have always appealed to me, as have those of Dr. Dionysus Lardner, who in 1823 advised that "Rail travel at high speed is not possible because passengers, unable to breathe, would die of asphyxia."[16]

I quote these gentlemen to remind that we cannot begin to imagine or comprehend where the onward march of discovery and technology will take us in the decades ahead. My words have offered a snapshot of the remarkable doors the Internet has opened and the formidable new challenges the Internet era has posed for the work of intelligence. It is an era in which the U.S. Intelligence Community continues to set aside old practices in favor of dramatically new ways of doing business. This comes at a time when both decision makers and military commanders recognize the heightened priority and the central importance of good intelligence in providing for the wellbeing, the security, and the defense of the United States.

Thank you.

End Notes

1. *Most Secret and Confidential,* Stephen E. Maffeo, Naval Institute Press, Annapolis, Maryland, 2000, pp 68-69.

2. Predator, A Global Option, General Atomics Aeronautical Systems Fact Sheet, General Atomics Aeronautical Systems, Inc., San Diego, California.

3. The Birth of Internet, http//www.lk,cs.ucla.edu/LK/Inet/birth.htrr.

4. The Living Internet, http.//www.livinginternet.com/i/ii_darpa.htr, p.1.

5. *The Information Resources Policy Handbook,* Edited by Benjamin M. Compaine and William H. Read, The MIT Press, Cambridge, Massachusetts, 1999, p. 22.

6. Fredrick Thomas Martin, *TOP SECRET INTRANET,* Prentice Hall, Upper Saddle River, New Jersey, 1999, pp. 6-7.

7. *ibid,* p. xliii.

8. *ibid,* pp 53-56.

9. http.//www.In-Q-Tel.com/about.htn.

10. "In-Q-Tel: A New Partnership Between the CIA and the Private Sector," Rick E. Yannuzzi, *Defense Intelligence Journal,* Volume 9, Number 1, Winter 2000, pp. 29-30.

11. *Strategic Intent,* Director of Central Intelligence, March 1999, Washington, D.C., p.1.

12. *Joint Vision 2010,* Chairman of the Joint Chiefs of Staff, Washington D.C., 1996, p.16.

13. LtGen Michael V. Hayden, USAF, Address to Kennedy Political Union of American University, 17 February 2000, p.2.

14. See Carmen A. Medina, "What to Do When Traditional Models Fail," *Studies in Intelligence,* Volume 45, No. 4, 2001, pp. 35-40.

15. "National Intelligence Support Teams," James M. Lose, *Studies in Intelligence,* Winter 1999-2000 Unclassified Edition, pp. 87-88.

16. Norman R. Augustine, "Socio-engineering (And Augustine's Second Law Thereof)," lecture presented at the University of Colorado Engineering Centennial Convention, 1 October 1993, p.1.